We claim:

1. A method for establishing a secure transmission channel from software of a first node to software of a second node comprising:

sending a key, identification of the first node, and identification of the second node from hardware of the first node to hardware of the second node;

receiving the key, identification of the first node, and identification of the second node by the hardware of the second node;

verifying the identification of the first node and the identification of the second node at the hardware of the second node; and,

storing the key at the hardware of the second node.

2. The method of claim 1, further initially comprising:

creating the key at the software of the first node; and,

storing the key at the hardware of the first node.

3. The method of claim 1, wherein each of the first node and the second node comprises one or more partitions, each partition corresponding to an operating system instance.

4. The method of claim 3, wherein the software of the first node comprises a process running in one of the one or more partitions of the first node.

5. The method of claim 4, wherein the identification of the first node comprises at least one of identification of the process running in the one of the one or more partitions of the first node, and identification of the one of the one or more partitions of the first node.

6. The method of claim 3, wherein the identification of the second node comprises at least one of identification of a process running in one of the one or more partitions of the second node, and identification of the one of the one or more partitions of the second node.

7. The method of claim 1, wherein each of the hardware of the first node and the hardware of the second node comprises a connection management mechanism.

8. The method of claim 1, wherein verifying the identification of the first node and the identification of the second node at the hardware of the second node comprises verifying the identification of the first node and the identification of the second node in a channel state table accessible by the hardware of the second node and accessible by the software of the second node.

9. The method of claim 1, wherein storing the key at the hardware of the second node comprises storing the key in a key table accessible by the hardware of the second node but inaccessible by the software of the second node.

10. The method of claim 1, further comprising:

creating a message at the software of the second node;

sending the message, the key, the identification of the first node, and the identification of the second node from the hardware of the second node to the hardware of the first node;

receiving the message, the key, the identification of the first node, and the identification of the second node by the hardware of the first node;

verifying the key at the hardware of the first node; and,

processing the message at the software of the first node.

11. A computerized system comprising:

a first connection management mechanism at a first node to maintain first keys for secure communication to first processes running in one or more first partitions of the first node from second processes running in one or more second partitions of a second node, the first keys inaccessible by the first processes, each first key used for secure communication to one of the first processes from one of the second processes; and,

a second connection management mechanism at the second node to maintain second keys for secure communication to the second processes from the first processes, the second keys inaccessible by the second processes, each second key used for secure communication to one of the second processes from one of the first processes.

12. The system of claim 11, further comprising:

a first key table at the first node to store the first keys, the first key table accessible by the first connection management mechanism but inaccessible by the first processes; and,

a second key table at the second node to store the second keys, the second key table

accessible by the second connection management mechanism but inaccessible by the second processes.

13. The system of claim 11, further comprising:

a first connection table at the first node and accessible by the first connection management mechanism and the first processes, the first connection table having a number of first entries, each first entry identifying one of the first processes, one of the second processes with which the one of the first processes is securely communicating, and one of the one or more second partitions in which the one of the second processes is running; and,

a second connection table at the second node and accessible by the second connection management mechanism and the second processes, the second connection table having a number of second entries, each second entry identifying one of the second processes, one of the first processes with which the one of the second processes is securely communicating, and one of the one or more first partitions in which the one of the first processes is running.

14. The system of claim 13, further comprising:

a first key table at the first node having a number of first key entries, each first key entry corresponding to a first entry of the first connection table and storing one of the first keys, the first key table accessible by the first connection management mechanism but inaccessible by the first processes; and,

a second key table at the second node having a number of second key entries, each second key entry corresponding to a second entry of the second connection table and

storing one of the second keys, the second key table accessible by the second connection management mechanism but inaccessible by the second processes.

15. An article comprising:

a computer-readable signal-bearing medium; and,

means in the medium for maintaining keys for secure communication to first processes running in one or more first partitions of a first node from second processes running in one or more second partitions of a second node, the keys inaccessible by the first processes, each key used for secure communication to one of the first processes from one of the second processes.

16. The article of claim 15, wherein the means in the medium is further for storing the keys in a key table inaccessible by the first processes.

17. The article of claim 15, wherein a connection table at the first node is accessible by the means in the medium and the first processes, the connection table having a number of entries, each entry identifying one of the first processes, one of the second processes with which the one of the first processes is securely communicating, and one of the one or more second partitions in which the one of the second processes is running.

18. The article of claim 17, wherein a key table at the first node is accessible by the means in the medium but inaccessible by the first processes, the key table having a number of key entries, each key entry corresponding to an entry of the connection table and storing one of the keys.

19. The article of claim 15, wherein the medium is a recordable data storage medium.

20. The article of claim 15, wherein the medium is a modulated carrier signal.